Quokka

GUIDE

Mobile Application Security

Best Practices for Fintech Apps

Quokka

Guide

Mobile Application Security Best Practices for Fintech Apps

Fintech, short for financial technology, is a sector of the economy that leverages technology to deliver innovative solutions and services within the financial services industry. This includes areas such as payments, banking, investments, and insurance. Today, fintech applications are revolutionizing the financial services industry, allowing for greater efficiency, convenience, and security.

Fintech applications are increasing customers' credit and financial literacy in a number of ways. They enable customers to quickly access personalized advice tailored to their individual circumstances and goals. This can help customers better understand the different products available to them, enabling them to make informed decisions about their finances.

Cybercriminals are increasingly targeting fintech applications due to the large amounts of sensitive data and financial information that they store. They employ a variety of attack methods in order to gain access to this data, such as phishing attempts, malware, and even social engineering. The ultimate goal of cybercriminals is typically financial gain by stealing money from accounts or selling stolen data on the black market. Other types of information they are after include personally identifiable information (PII) such as names and addresses, as well as credit card numbers and passwords. By obtaining this data, criminals can use it for identity theft or other fraudulent activities.

Security Standards for Fintech Applications

When building fintech applications, it is critical to ensure proper security standards are in place in order to protect customer data and financial information. Fintech applications inherently need a lot of PII for these apps to perform their intended functions. By adopting proper security measures, developers can help ensure their applications remain safe and secure for all users. Some of the fundamental security standards that should be considered include personal data protection, data encryption, role-based access control, secure application logic, and understanding of compliance and regulatory requirements.

Understanding how a customer interacts with the application and preparing appropriate safeguards for handling personal data can help organizations and development teams make smarter decisions about security protocols and access.

Ask yourself these three simple questions:

1. **Does this application make sure customer data is always encrypted at rest and in transit (on the device or elsewhere)?**
2. **Does this application verify the trustworthiness of the device it is being used on?**
3. **Does the application include appropriate security measures to protect the data it handles, such as SSL pinning?**

Building a Secure Fintech Application Step-by-Step

By following these steps, developers can help ensure their applications remain safe and secure for all users while protecting sensitive customer data from malicious actors and breaches of security protocols.

Step 1

Establish secure coding standards. Developing secure code is the cornerstone of any reliable fintech application. To ensure this, developers must establish and follow secure coding standards and best practices, such as avoiding input validation errors, using data encryption to protect sensitive information, enforcing the principle of least privilege, and avoiding hard-coding credentials.

Step 2

Perform mobile application security testing where you scan for libraries' vulnerabilities dynamically and statically. Mobile applications are vulnerable to malicious attacks, so they must be tested for potential vulnerabilities such as SQL injection and data leakage, but it is also important to scan for true vulnerabilities, which are exploitable weaknesses. Security testing should include both manual and automated testing. Testing should be conducted regularly to identify any deficiencies in the code that malicious actors could exploit.

Step 3

Implement user authentication measures. User authentication is an important security measure that requires users to provide multiple forms of verification before accessing an account or carrying out transactions. This helps protect users from potential fraudulent activities and protect their financial information from theft. Implementing two-factor authentication (2FA) can also help further verify user identity and increase the security of accounts.

Step 4

Implement data privacy and protection measures. Data privacy is essential for fintech applications as they store a large amount of personal and financial data. It is important that customers' personal information is collected, stored, and handled in accordance with applicable laws and regulations such as GDPR. Encrypting data can also help protect user information from being accessed by unauthorized parties or malicious actors.

Step 5

Apps use cloud servers as well as API servers to serve the users with data from the backend. It is important to ensure that this part of the mobile application is secured since most of the data is stored here. Access must be strictly monitored to prevent any potential cyber threats while also eliminating all weak spots within our infrastructure.

Q-MAST and Fintech Applications

Mobile application security testing, including Q-MAST, is the advanced analysis of applications in development or publicly available through the Google(R) Play or Apple App Store. Security testing for mobile applications typically involves checking for vulnerabilities such as SQL injection, data leakage, and other malicious activities. These tests can also be used for vulnerability detection and to identify any weaknesses in the code that may allow an attacker to gain access to sensitive data or carry out malicious actions. When an application is tested during the development lifecycle, teams or individuals responsible for code and functionality can use automated testing to “break” their application during each sprint. As the application inches closer to publication, the development team will be able to share a software Bill of Materials (SBOM) with any internal application security leadership, showcasing the discrete components that make up the application and if it is subject to known vulnerabilities.

For applications readily available on the public app stores, organizations can deploy mobile application security testing to confirm that their application security protocols remain in place, even after multiple version releases. This safeguard ensures nothing is released to the App Store that may skip regular DevSecOp pipeline checks. As the device’s technology and functionality expand, fintech applications must remain true to their security foundations while addressing additional functionality. By conducting thorough security tests and implementing appropriate security measures, developers can help ensure the safety and confidentiality of customer information stored within the application.

Quokka’s Testing Process

Quokka's Q-MAST solution goes beyond the capabilities of a traditional Software Composition Analysis (SCA) for Android & iOS applications. We analyze how libraries operate within a given context and identify potential encryption or privacy issues. Our dynamic analysis tests go beyond industry standard OWASP CycloneDX reports, uncovering weaknesses and vulnerabilities not yet known to the public. We ensure your app is up to standard when it comes to security protocols like encryption standards and information sharing locations – ensuring you stay in line with your own privacy policy.

Our innovative approach to analyzing apps yields unparalleled insights into the security of an app. With our detailed information, we can detect a wide array of potential threats and trace back their origins with definitive accuracy - even in cases where running an application is impossible. We take pride in both developing tech that has been independently tested and publicly validated as well as going through rigorous peer-reviewing processes for each product's effectiveness.

Quokka Threat Scores

Our Q-MAST technology enables organizations to effectively measure the security and privacy preparedness of their applications. We’ve assigned “threat scores” to applications, a higher score on our threat scale means your system may be less equipped for protection, while a lower rating indicates more readiness against threats.